

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3-5, 7, 9, 11 and 13-18 are pending in the application. Claims 1, 9 and 13 are amended; and Claims 8 and 12 are canceled without prejudice or disclaimer by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.¹ No new matter is presented.

In the Final Office Action of March 19, 2009, Claims 1, 3-5, 7-9 and 11-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. 6,248,946 to Dwek in view of U.S. Pub. 2001/0051996 to Cooper et al. (herein, Cooper).

In response to the above noted rejection under 35 U.S.C. § 103, Applicant respectfully submits that amended independent Claims 1, 9 and 13 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites, in part, a user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

- ... transmitting, from said mobile information terminal to said authentication server, a request to connect to the authentication server;
- transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature;
- verifying an identity of the authentication server at the mobile information terminal based on the received certificate;
- generating, at a Web browser of the mobile information terminal, a secret key based on a result of the verification;
- encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server;
- transmitting the encrypted secret key from the mobile information terminal to the authentication server;

¹ e.g., specification at Fig. 19 and pp. 33-35.

receiving, at the authentication server from said mobile information terminal, the unique identification information as encrypted by said secret key at the Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network ...

Independent Claims 9 and 13, while directed to alternative embodiments, are amended to recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 9 and 13.

In rejecting the arguments presented in the previous response that the applied references fail to teach or suggest transmitting the unique identification information as encrypted by a predetermined encryption algorithm by a Web browser installed of the mobile information terminal, the Advisory Action of May 28, 2009 asserts that “the encryption of any transmitted information, including any identifying information, is clearly taught throughout Cooper, in particular paragraphs 39, 43, 52 and 58.”

This cited portion of Cooper, however, fails to teach or suggest the authentication process that leads to the generation of the secret key used encrypt the unique identification information, as recited in amended independent Claims 1, 9 and 13.

More particularly, paragraph [0039] of Cooper describes a generic configuration of a conventional computer, and paragraph [0043] describes that a process of using a private key to generate a message that, when decrypted using a public key, validates that the message was generated using an individual’s private key. Further, paragraph [0052] of Cooper describes that Secure Sockets Layer (SSL) may be used to facilitate a Virtual Private Network (VPN) connection, and paragraph [0058] describes the before content is transferred via the VPN that it may be encrypted.

Cooper, therefore, does appear to describe that data may be encrypted prior to being transmitted via the VPN, but fails to teach or suggest the claimed features leading to the generation of a secret key used to encrypt transmitted unique identification information, as recited in amended Claim 1. Particularly, Cooper fails to teach or suggest transmitting, from a mobile

information terminal to an authentication server, a request to connect to the authentication server; transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature; verifying an identity of the authentication server at the mobile information terminal based on the received certificate; generating, at a Web browser of the mobile information terminal, a secret key based on a result of the verification; encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server; transmitting the encrypted secret key from the mobile information terminal to the authentication server; and receiving, at the authentication server from said mobile information terminal, the unique identification information as encrypted by said secret key at the Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network, which are all features required by amended independent Claim 1.

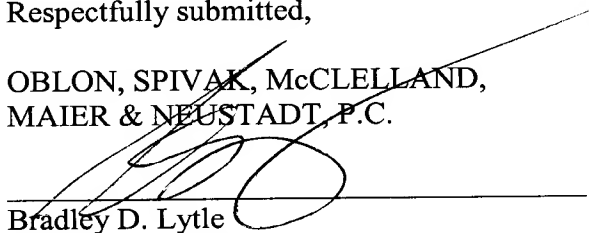
Further, Dwek fails to remedy the above noted deficiencies of Cooper.

Accordingly, for at least the reasons discussed above, Applicant respectfully requests that the rejection of Claims 1, 3-5, 7, 9, 11 and 13-18 under 35 U.S.C. § 103 be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-5, 7, 9, 11 and 13-18 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Andrew T. Harry
Registration No. 56,959